PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-036517**
(43)Date of publication of application : **09.02.2001**

(51)Int.CI. H04L 9/08
G09C 1/00
H04N 5/44
H04N 7/08
H04N 7/081
H04N 7/16
H04N 7/167

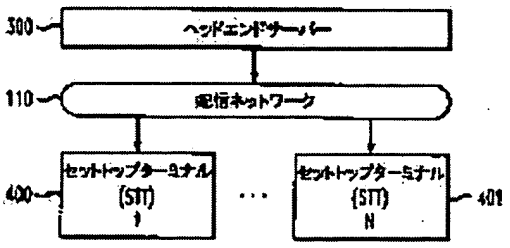
(21)Application number : **2000-135069**
(22)Date of filing : **08.05.2000**

(71)Applicant : **LUCENT TECHNOL INC**
(72)Inventor : **BLEICHENBACHER DANIEL**
WOOL AVISHAI

(30)Priority
Priority number : **99 307643** Priority date : **07.05.1999** Priority country : **US**

(54) METHOD FOR TRANSMITTING PROGRAM TO LIMIT ACCESS TO END USER AND METHOD FOR DECODING ENCRYPTED PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system to limit access to contents of transmission program such as television program.
SOLUTION: A transmitter or a head end server is used by a service provider to transmit encrypted programming contents to one or a plurality of customers. A program identifier (p) used to identify a program is transmitted to the customers together with programming contents. Each customer uses a set-top terminal or an interpretation key to provide a limited access to transmission multimedia information as other device. The set-top terminal 400 or the like receives entitlement information corresponding to a package of one or a plurality of programs that can normally be received for a period from a head end.



LEGAL STATUS
[Date of request for examination] 13.08.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The step which assigns the program identifier which is the approach of transmitting the program which can carry out access restriction to an end user, and has (A) binary value to said program, (B) The step which enciphers said program by using the step which defines at least one master key, and the program key obtained by applying at least one Hash Function to said master key based on the binary value of the (C) aforementioned program identifier, (D) Approach characterized by having the step which sends said enciphered program to said end user with said program identifier.
[Claim 2] Said program identifier is an approach according to claim 1 characterized by applying one of said the Hash Functions to each location of n bits of said program identifier according to the bit value to which it becomes from n bits and said program identifier corresponds.
[Claim 3] (E) The approach according to claim 1 characterized by having further the step which provides said end user with entitlement information based on the set of the program acquired by said end user.
[Claim 4] The approach according to claim 3 characterized by including some key trees based on the set of the program acquired by said end user in said entitlement information.
[Claim 5] Said end user is an approach according to claim 3 characterized by using said program identifier in order to obtain said program key from said memorized entitlement information.
[Claim 6] Said program identifier is an approach according to claim 1 characterized by interleaving with transmission of said encryption program.
[Claim 7] Said program identifier is an approach according to claim 1 characterized by being transmitted on a control channel.
[Claim 8] The approach characterized by to have the step enciphered using the program key which is the approach of transmitting a program to two or more end users, and was obtained by applying a Hash Function to the master key based on the binary value of each bit position of said program identifier for the program which has (A) program identifier recurrently, and the step which transmits the program which carried out (B) encryption, and said program identifier to said end user.
[Claim 9] Said program identifier is an approach according to claim 8 characterized by applying said Hash Function to each location of n bits of said program identifier according to the bit value to which it becomes from n bits and said program identifier corresponds.
[Claim 10] (C) The approach according to claim 8 characterized by having further the step which provides said end user with entitlement information based on the set of the program acquired by said end user.
[Claim 11] The approach according to claim 10 characterized by including some key trees based on the set of the program acquired by said end user in said entitlement information.
[Claim 12] Said end user is an approach according to claim 10 characterized by using said program identifier in order to obtain said program key from said memorized entitlement information.
[Claim 13] Said program identifier is an approach according to claim 8 characterized by interleaving with transmission of said encryption program.
[Claim 14] Said program identifier is an approach according to claim 8 characterized by being transmitted on a control channel.
[Claim 15] It is the approach of transmitting the program corresponding to at least one program package to two or more end users. (A) The step which provides said end user with entitlement information based on the set of the program acquired by said end user, (B) The step enciphered using the program key obtained by applying a Hash Function to the master key based on the binary value of each bit position of said program identifier for the program

which has a program identifier recurrently, (C) Have further the step which transmits said program identifier to said end user with the enciphered program, and if said end user is a just user of said program Said end user is an approach characterized by obtaining said program key from the memorized entitlement information.
[Claim 16] Said program identifier is an approach according to claim 15 characterized by applying one of said the Hash Functions to each location of n bits of said program identifier according to the bit value to which it becomes from n bits and said program identifier corresponds.
[Claim 17] The approach according to claim 15 characterized by including some key trees based on the set of the program acquired by said end user in said entitlement information.
[Claim 18] Said end user is an approach according to claim 15 characterized by using said program identifier in order to obtain said program key from said memorized entitlement information.
[Claim 19] Said program identifier is an approach according to claim 15 characterized by interleaving with transmission of said encryption program.
[Claim 20] Said program identifier is an approach according to claim 15 characterized by being transmitted on a control channel.
[Claim 21] The step which receives the entitlement information which is the approach of decoding the enciphered program and contains at least one middle key from a key tree based on the set of the program which said customer acquired from the provider of the (A) aforementioned program, (B) The encryption program enciphered by the program key, and the step which receives a program identifier, (C) Approach characterized by having the step which obtains said program key from the part said program identifier and said key tree were remembered to be, and the step which decodes said encryption program using the (D) aforementioned program key.
[Claim 22] It is the approach according to claim 21 which said program identifier consists of n bits, and said master key is arranged on the root of said key tree, and is characterized by generating said key tree when said key tree applies a Hash Function to each node until the tree level of n is made.
[Claim 23] It is the approach of decoding the enciphered program. From the provider of the (A) aforementioned program The step which receives the entitlement information which contains at least one middle key from the key tree based on the set of the program which a customer acquires, (B) The encryption program enciphered by the program key, and the step which receives a program identifier, (C) The step which obtains said program key from the part the key tree was remembered to be from said program identifier and said middle key by applying a Hash Function to said middle key recurrently based on the binary value of said program identifier, (D) Approach characterized by having the step which decodes said encryption program using said program key.
[Claim 24] It is the approach according to claim 23 which said program identifier consists of n bits, and said middle key corresponds to the intermediate node in the level r of said key tree, and is characterized by carrying out n-r time application of said Hash Function at said middle key.
[Claim 25] The memory which is the system which transmits the program which restricts access to an end user, and memorizes the (A) master key and a computer readout possible code, (B) It has the processor connected with said memory in actuation. This processor (a) The program identifier which has a binary value is assigned to said program. (b) Define at least one master key and said program is enciphered using a program key by applying at least one Hash Function to said master key based on the binary value of the (c) aforementioned program identifier. (d) System characterized by constituting so that an encryption program may be transmitted to said end user with said program identifier.
[Claim 26] The memory which is the system which transmits the program to which access to an end user was restricted, and memorizes the (A) master key and the code which can be computer read, (B) It has the processor connected with said memory on actuation. Said processor (a) The program key obtained by applying a Hash Function to a master key recurrently based on the binary value of each bit position of said program identifier is used. The system characterized by constituting so that this program that enciphered this program that has a program identifier and was enciphered by the (b) aforementioned end user, and said program identifier may be transmitted.
[Claim 27] The memory which is the system which decodes the enciphered program and memorizes the (A) master key and the code which can be computer read, (B) It has the processor connected with said memory on actuation. Said processor (a) The entitlement information containing the part of the key tree based on the set of the program acquired by said customer is received from the provider of this program. (b) The encryption program enciphered by the program key and a program identifier are received. (c) System characterized by obtaining said program key from said part said program identifier and said key tree were remembered to be, and constituting so that said encryption program may be decoded using the (d) aforementioned program key.
[Claim 28] It is the medium by which the code means which can be computer read was mounted and which can be

computer read. This means that can be computer read assigns the program identifier which has (a) binary value at the time of actuation to a program. (b) Define at least one master key and the program key obtained by applying at least one Hash Function to said master key based on the binary value of the (c) aforementioned program identifier is used. The medium which is characterized by transmitting this program that enciphered this program and was enciphered with the (d) aforementioned program identifier to an end user and which can be computer read.
[Claim 29] It is the medium by which the code means which can be computer read was mounted and which can be computer read. This means that can be computer read receives the entitlement information containing the part of the key tree based on the set of the program acquired by the (a) aforementioned customer at the time of actuation from the provider of this program. (b) The encryption program enciphered by the program key and a program identifier are received. (c) Medium which is characterized by obtaining said program key from said part said program identifier and said key tree were remembered to be, and decoding said encryption program using the (d) aforementioned program key and which can be computer read.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the system which transmits the program decoded with the memorized entitlement information using the program identifier used by the set top terminal, in order to obtain a decode key required to decode a program especially about the system which restricts access to the contents of transmitting programming.
[0002]
[Description of the Prior Art] It is still more important that a service provider like a cable television operator or a digital satellite service operator offers the package of the channel to which a majority of a television viewer's population is satisfied, or a program as the number of channels with an available television viewer increases and the range of the available contents of programming increases in number by such channel. Generally development of the package with which a customer is provided is a marketing function. A service provider is wanted to offer the package of various sizes generally. For example, they are all programs, the combination between them, etc. from one program.

[0003] A service provider usually broadcasts a television program from the transmitter called a "head end" to many customers. Each customer is usually concerned with a part of programming to receive. For example, in a broadcast environment, any man can receive programming transmitted with a suitable receiver like an antenna or a satellite disk. In order to restrict access of a program only to the normal customer who purchased the package, a service provider usually enciphers a transmitting program and contains 1 or two or more code machines in a customer. A set top terminal (STT) is offered. By such approach, a set top terminal receives encryption transmission and the program which a customer looks at is enciphered. Nothing is carried out but this.
[0004] In order that the confidentiality memorized in the set top terminal may make piracy of high information min, a set top terminal is usually equipped with a secure processor or secure memory. This secure memory has the capacity of several kilobits order, and memorizes a code key. Generally secure memory is not volatility but tamper REJISUTANTO. Moreover, secure memory has that it can write [much] in and can carry out the repro gram of the key for every accounting period. Since the secure memory capacity of the conventional set top terminal is restricted, the number of the keys memorized will be restricted and the number of the packages which a service provider offers will also be restricted. The number of the programs which a service provider broadcasts to the accounting period of a moon unit may usually be the order of 200,000.
[0005] The conventional set top terminal has a thing containing bit VEKUTORU which has a bit entry corresponding to each package of the program which a service provider offers. If a specific customer is the normal addressee of a package, the bit entry in the bit vector memorized in a set top terminal will be set to "1." After that, all the programs that a service provider transmits are enciphered by one key. If a program is received, a set top terminal will judge whether the bit entry which accesses and corresponds to a bit vector is set. If the bit entry is set, as for a set top terminal, a program will be decoded using one memorized code machine.
[0006] Although it seems to a theory top that flexibility is attained by the bit vector method by offering one bit entry to each package (a package consisting of one program generally), the die length of a bit vector is not practical in the system which transmits many programs to one accounting period. Moreover, the access control in such a system is exclusively given by the entry in a bit vector, and is not code-like (cryptographic). Therefore, if a customer can write in a bit vector and can set all bits to "1", a customer will be able to access all programs.
[0007] Moreover, a program is divided into each package and there are some as which all the programs in a package are enciphered using the same key. Each package corresponds to one television channel. A set top terminal

memorizes the decode key to each package the customer of whose is a normal addressee. Therefore, if a program is included in two or more packages, that program must be broadcast again for corresponding each package of every, and will be enciphered in this the transmission of each by the code key corresponding to a specific package. Although it is cryptography-like [an access control], by the overhead about broadcasting programming again repeatedly, it will not be realistic, and will carry out arranging the same program as much packages, and flexibility will be restricted in the design of the package of a program.

[0008] although the conventional system which encipher such contents of a program and be transmit be comparatively successful about restrict access only to a normal customer , it have not make it possible to provide a customer with the package with which a large number which include much programs , without make an overhead increase fairly differ , without a service provider like a television network exceed the secure memory capacity to which the set top terminal be restricted . The cryptography-approach and equipment which restrict access to the contents of transmitting programming to the "Vspace system" indicated by the United States patent applications 08/912186 (August 15, 1997 application) are indicated.

[0009] Each program in a Vspace system is enciphered by the head end server before transmission using the program key kP. Each program key is the linearity combination of the set with which the master key M was defined. The program identifier which identifies a program is transmitted with the contents of encryption programming. A customer's set top terminal can obtain a decode key only from the entitlement information recorded on the program identifier p which received, and the front. A Vspace system offers a cryptography-access-control mechanism, enabling the package which is supple, without extending a program header fairly (only a program identifier being transmitted with a program). It is because it is not necessary to broadcast a program again for corresponding each package of every.

[0010]

[Means for Solving the Problem] Generally, the contents of programming enciphered by 1 or two or more customers by the service provider using the transmitter thru/or the head end server are transmitted. The program identifier p used for identifying a program is transmitted to a customer with the contents of programming. Each customer has other devices in which access restricted to transmitting multimedia information using the set top terminal thru/or the decode key is given. A set top terminal receives 1 which can receive to normal at a period with a customer, or the entitlement information corresponding to the package of two or more programs from a head end.

[0011] Each program is enciphered by the head end server before transmission using the program key kp. the program key kp of an individual -- the program -- unique -- making . In addition to transmission of the enciphered program, a head end server transmits the program identifier p to a set top terminal. A set top terminal obtains a decode key required to decode a program using the program identifier p which received with the memorized entitlement information. In this approach, if a customer is the normal user of a specific program, a set top terminal can obtain the program key kp enciphered using the information memorized and received, and can decode the program enciphered using that program key kp after that. In an example, the program identifier p can be interleaved to a part of program, and can be transmitted on a separate exclusive control channel.

[0012] Each of k-bit program key kp used for enciphering a transmitting program can be obtained by applying 1 or two or more pseudo-random Hash Functions to a master key m. As an example, Hash Function H which doubles die length can be used. Therefore, Hash Function H takes a k bit binary value, and makes the binary value of the die length of 2k. The output of Hash Function H can be expressed as pair H0 of k-bit binary value as H1. Here, H0 can be identified as a left half of the output of the Hash Function concerned, and H1 can be identified as a right half of the output of the Hash Function concerned.

[0013] As an example, the program key kp can be obtained according to the binary value to which each bit position of the program identifier p corresponds by applying recurrently Hash Functions H0 or H1 to a master key. Therefore, if the program identifier p consists of m bits, one side of Hash Functions H0 or H1 will be applied to each bit position of n of the program identifier p according to the bit value to which the program identifier p corresponds. First, one side of Hash Functions H0 or H1 is applied to a master key according to the binary value which is the leftmost digit bit of the program identifier p. After that, according to the binary value of a corresponding bit, one side of Hash Functions H0 or H1 is applied to the result of a pre- hash operation to each remaining bit position (n-1). Count of the program key kp can be expressed as follows.

[Equation 1]

$$K_p = H_{p_n}(\ldots H_{p_2}(H_{p_1}(m))\ldots)$$

[0014] Such a hash operation can be expressed in relation to n level binary tree T (called a key tree) by which the root 2 master key m of a tree is arranged. A tree is generable by applying Hash Functions H0 and H1 to each node until a desired number of tree-level (n) is made. The program key kp corresponds to the leaf (leaf) node in the bottom (bottom) level of a tree. The binary index (the same the program identifier [And] p) corresponding to each program key kp corresponds to the pass (way) which passes along the key tree from the root to a desired leaf node. Therefore, the index thru/or label of Node u is connection of the label on H on the pass from the root to Node u. T (u) can calculate any key of the program in subtree T (u) by carrying out time (n-r) actuation of the Hash Function to the internal node u (u1, ..., ur) in depth r in the subtree which makes Node u the root, i.e., the key tree which has the partial program identifier p showing the set of the program identifier p corresponding to the leaf in the subtree of Node u.
[0015]
[Embodiment of the Invention] Drawing 1 has shown the network environment which transmits video, an audio, and encryption multimedia information like data to 1 or two or more customers who have the set top terminals 400-401 through 1 or two or more distribution networks 110 using a transmitter like the head end server 300 from a service provider. This head end server 300 argues in relation to drawing 3 in the bottom, and argues about the set top terminal 400 in relation to drawing 4 in the bottom. In this specification, a set top terminal includes any device in which access restriction is given to the multimedia information transmitted using the decode key. For example, a computer configuration and a communication link device are included. A service provider may download the software which a set top terminal performs. A network 110 can be made into the wireless broadcasting network which distributes contents of programming like digital satellite service (DSSTM), a cable television network (CATV), a public switching network (PSTN), an optical network, ISDN, and a cable network like the Internet.
[0016] The set top terminal 400 receives entitlement information intermittently from the head end server 300, and enables a customer to access the program whose customer is a registered user between a certain time intervals (for example, accounting period). In this specification, a package is the set of a predetermined program and a certain program can belong to 1 or two or more packages. A program means all of continuous multimedia transmission of the episode of television, or specific die length like a movie. Entitlement information is downloadable in the set top terminal 400 from the head end server 300 using which suitable secure one way or bidirectional protocol.
[0017] Program key and program identifier each transmitting program is enciphered by the head end server 300 using the program key kp. This program key kp can be made unique to a program. Suitable encryption and a security technique are indicated by reference, B.Schneier, and Applied Cryptography (2d ed.1997). In addition to transmission of an encryption program, the head end server 300 also transmits a n bit program identifier to the set top terminal 400. This is used by the set top terminal 400 with the memorized entitled information, and as shown in a detail, it obtains a decode key required to decode a program in the bottom.
[0018] The program identifier p is not chosen as arbitration so that the item of the bottom entitled assignment of the program identifier to a program may explain. In a desirable example, the program identifier p can consist of the 32-bit value transmitted in the ECM field specified to MPEG-2 criterion. In this case, if it is the registered user of the program of specification [a customer], the set top terminal 400 can obtain the program key kp from the information memorized and received, and it can use the program key kp so that an encryption program may be decoded after that.
[0019] According to the further description of this invention, each of the k-bit program key kp used for an encryption transmitting program can be obtained by applying 1 or two or more pseudo-random Hash Functions to a master key m. Explanation of a suitable pseudo-random Hash Function is indicated by reference and O.Goldreich et al. and "How to Construct Random Functions" J.ACM and 33:792-807 (1986).
[0020] As an example, it is secure in cryptography, and the Hash Function which doubles die length is used as follows.
H: {0, 1} k->{0, 1}2k -- here, k is the die length of the program key kp. Therefore, Hash Function H takes the binary value of k bits, and makes the binary value of die-length 2k. The output of this Hash Function H can be expressed as pair H0 of a k bit binary value as H1. Here, H0 is the left-hand side one half (left-hand side digit bit) of the output of Hash Function H, and is H. {1} is the right-hand side one half (right-hand side digit bit) of the output of Hash Function H. H0 and H1 can be called a separate Hash Function.
[0021] If it is k= 160, H can be specified using secret hash standard SHA-1 which is indicated by reference, Secure Hash Standard, National Institute of Standards and Technology, NIST FIPS PUB 180-1, and U.S.Dept.of Commerce (April, 1995). That is, H0 is set to SHA-1 (x||0), and H1 turns into SHA-1 (x||1). Here, 0 and 1 are the bit strings of all the bit strings 1 of 0 altogether, respectively.

[0022] The program key kp can be obtained by applying recurrently 1 or two or more Hash Functions to a master key m according to the binary value of the program identifier p. As an example, the program key kp can be obtained by applying recurrently one side of Hash Functions H0 or H1 to a master key m according to the binary value of each bit position of the program identifier p. Generally, if the program identifier p consists of n bits, according to the bit value to which the program identifier p corresponds, one side of Hash Functions H0 or H1 will be applied to each of the bit position of n of the program identifier p (it starts from a leftmost bit).
[0023] One side of Hash Functions H0 or H1 is first applied to a master key according to the binary value which is a leftmost digit bit. After that, according to the binary value which is the bit to which one side of Hash Functions H0 or H1 corresponds, it is applied to the result of pre- hash actuation to each remaining bit position (n-1). This hash actuation can be expressed as follows so that the item of a title called lower "key tree" may explain.
[Equation 2]

$$K_p = H_{p_n}(\ldots H_{p_2}(H_{p_1}(m))\ldots)$$

[0024] As mentioned above, the head end server 300 transmits the program identifier p with an encryption program. Therefore, if the program identifier p is given, the set top terminal 400 must obtain the program key kp used for decode of a receiving agent. As mentioned above, the program key kp can be obtained by applying recurrently 1 or two or more Hash Functions to a master key m according to the binary value of the program identifier p. The program key kp must be obtained by a customer's set top terminal 400, using indirectly the memorized entitlement information and the program identifier p which received which is explained in the bottom.
[0025] As explained on the key tree, the program key kp can be obtained by using recurrently 1 or two or more Hash Functions for a master key m according to the binary value of the program identifier p. The k-bit single master key m is used. The bit of the program identifier p can be expressed as p= (p1, ..., pn). Here, p1 is a leftmost digit bit and is a rightmost digit bit. The cryptographic key kp to the program which has the program identifier p can be defined as follows.
[Equation 3]

$$K_p = H_{p_n}(\ldots H_{p_2}(H_{p_1}(m))\ldots)$$

[0026] Hash actuation can be expressed as a perfect n level binary tree T like the key tree 200 shown in drawing 2 . The key tree 200 shown in drawing 2 corresponds to the example of mounting which has the program identifier p which consists of a triplet. As shown in drawing 2 , a master key m is arranged on the root 210 of a tree 200. The program key kp corresponds to a leaf node like leaf nodes 240-247. The index corresponding to each program key kp shown in drawing 2 like the index 011 corresponding to the program key kp of the DERIFU node 243 shows the pass which lets the key tree 200 from the root 210 to a leaf node 243 pass. For example, the program key kp of 243 can be obtained by following with the left edge (H0) from the root 210, the right edge (H1) from a node 220, and the right edge (H1) from a node 232. That is, H1 is further applied for H0 to the 2nd hash result. The program key kp011 can be obtained.
[0027] Therefore, the label of a node u like a node 243 is what connected the label on the edge of the pass to Node u from the root 210. The label of each node can be specified by the program identifier p. Since the subtree which makes Node u the root is expressed, T (u) is used (namely, since the set of the program identifier p corresponding to the leaf in the subtree of Node u is expressed). The internal node u in depth r in the key tree 200 has the partial program identifier p (u1, ..., ur), and can calculate the key of which program in subtree T (u) to these. Any key of the program in the subtree of Node u is calculable by carrying out time (n-r) actuation of the Hash Function. Specifically, it uses so that the value of each bit of the low digit of (n-r) of the program identifier p may direct suitable Hash Functions H0 or H1. Therefore, the program key kp corresponding to Node u can function as an entitlement to all the programs in the subtree of Node u.
[0028] If Function H is a pseudo-random generator, mapping kp{0, 1} ->[n] {0, 1} k of the program key which the master key m parameterized is a pseudo-random function. This is indicated by reference, and O.Goldreich et al. and "How toConstruct Random Functions" J.ACM and 33:792-807 (1986).
[0029] System component drawing 3 is the block diagram showing the head end server's 300 AKI theque char. A head end shall be related with the service provider of the arbitration which transmits a television network, a cable employment person, a digital satellite service employment person, or the contents of encryption programming. For example the head end server 300, can mount with RS6000 server which manufactures, and can perform the function and actuation of this invention. The head end server 300 is equipped with related memory like a processor 310 and the

data storage device 320. A processor 310 may be mounted as a single processor and may be mounted as some processors which operate to juxtaposition. The data storage device 320 and ROM are made to memorize 1 or two or more instructions, and a processor 310 enables it to perform by taking out and interpreting.
[0030] As mentioned above, the data storage device 320 is equipped with the master key database 350 which memorizes a master key m. For example, a master key m can be updated like [for every accounting period]. Moreover, the data storage device 320 has the program database 500 so that it may explain in relation to drawing 5 in the bottom. The program database 500 presents the program identifier p and the related package corresponding to each program. moreover, drawing 7 R> -- the data storage device 320 has the entitlement information delivery process 700 and the program delivery process 800 so that it may explain in relation to 7 and 8.
[0031] Generally, the entitlement information delivery process 700 generates and distributes the entitlement information which each customer needs to accessing the program which is a registered user. Moreover, the program delivery process 800 obtains the program key kp based on the program identifier p assigned to the program, in order to encipher a program and to transmit by the program identifier p.
[0032] The communication link port 330 links the head end server 300 to each connected receiver like the set top terminal 400 which showed the head end server 300 to the network 110 at a bond and drawing 1 .
[0033] Drawing 4 is the block diagram showing the AKI theque char of the set top terminal 400. The set top terminal 400 can be mounted as a set top terminal (STT) corresponding to television, and it can be changed so that the function and actuation of this invention may be performed. The set top terminal 400 is equipped with a processor 410 and memory like data storage 420, and the communication link port 430, and operates by the same approach as the above hardware relevant to drawing 3 .
[0034] Data storage 420 is equipped with the entitlement database 600 memorizable into the secure part of data storage 420 so that it may explain in relation to drawing 6 in the bottom. The entitlement database 600 contains the part of the key tree 200 required in order that a customer may get the program key kp to the program which has an entitlement. Moreover, data storage 420 is equipped with Hash Functions H0 and H1 (440). Moreover, data storage 420 includes the decoding process 900 so that it may explain in relation to drawing 9 in the bottom. Generally, using the program identifier p received in order to obtain the program key kp, and the memorized entitlement information 600, in order to decode a program, the program key kp is used for the decoding process 900, and it decodes the program whose customer has an entitlement.
[0035] Drawing 5 shows the program database 500 which memorizes information on each program p transmitted by the head end server 300. This information is transmitted to for example, an accounting period with the program identifier p to which that program belongs and which packs and corresponds. The program database 500 holds two or more decodings like records 505-520. These are related with a different program, respectively. The program database 500 contains the program identifier p which corresponds in the field 535 including directions of the corresponding package with which the program belongs in the field 530 to each program identifier identified by the program name in the field 525.
[0036] Drawing 6 shows the entitlement database 600 containing the part of the key tree 200 required for a customer to get the program key kp to the program which has an entitlement. As mentioned above, T (u) expresses the set of the program identifier p corresponding to the leaf nodes 240-247 in the subtree which makes Node u the root, i.e., the subtree of Node u. For example, supposing a customer has an entitlement about receiving four programs corresponding to leaf nodes 240-243, entitlement information will consist of a middle key corresponding to a node 220. In this approach, if needed, suitable Hash Functions H0 and H1 (440) can be used in order to obtain the program key kp to each nodes 230, 232, 240-243 in the subtree of a node 220.
[0037] The entitlement database 600 shown by drawing 6 is a registered user who receives four programs corresponding to leaf nodes 240-243 (there is an entitlement), and is a registered user who receives two programs corresponding to leaf nodes 246-247. Therefore, the entitlement information recorded on the entitlement database 600 consists of a middle key corresponding to a node 220 and a node 236. nodes 220 and 236 -- it is alike, respectively, and it receives, and the entitlement information recorded on the entitlement database 600 has the middle key values kio and ki11, respectively, and has corresponding directions of the partial program identifier p. The approach by which the entitlement database 600 is generated by the entitlement information delivery process 700 based on the package of the program which the customer chose is explained in relation to drawing 7 in the bottom.
[0038] A small entitlement is establishable to the set of many programs of various sizes using the tree method of program packaging this invention. The target set S is established using the set of the program packed. The minimum set of a tree node with which a subtree covers the target set S correctly is obtained as follows.

[Equation 4]
$T(S)=Z\subseteq T$ ただし、$\bigcup_{u\in Z}T(u)=S$、かつ、$|Z|$ は最小であるように

[0039] The entitlement information over Package S is the set ki of the middle key held in the node of T (S). As shown in a top, the set top terminal 400 decodes the program in S (accepting it) correctly with the set of this key. Theoretically, the tree method of this invention can build the entitlement information over the target set S of which arbitration. furthermore -- however, if the program identifier p is assigned to arbitration, entitlement information will become so large that it is not allowed for the secure memory to which the set top terminal 400 was restricted.
[0040] a process -- as mentioned above, the head end server 300 performs the entitlement information delivery process 700 shown in drawing 7 , and generates and distributes the entitlement database 600 required for each user in order to access the program which is a registered user. As mentioned above, the entitlement database 600 consists of corresponding directions and the corresponding middle key value ki of a partial program identifier to each node of the key tree 200 required for a customer to get the program key kp to the program which is a registered user.
[0041] Therefore, the entitlement information delivery process 700 identifies first the program which the customer chose (710). After that, the entitlement information delivery process 700 finds minimum set [of a tree node] T (S). The subtree covers the target set S correctly. The target set S is disassembled to the maximum De Dis joint interval of the KONSEKYUTIBU program identifier p (720). Two program identifiers p are considered to be KONSEKYUTIBU when the integer over the binary expression is KONSEKYUTIBU.
[0042] And covering T (S) is found to each interval (730). The corresponding partial program identifier p held in the node of covering T (S) to Set ki and each interval of a middle key is generated (740). At the end, the generated entitlement information downloads to the set top terminal 400 with the head end server 300 (750), and program control is completed (760).
[0043] The number of the intervals in the target set S can be set to I (S). In order to calculate covering T (S) to the single interval of the program identifier p to the order of the tree node of n, the key tree 200 of depth n must be asked. Therefore, the time amount complexity of the entitlement information delivery process 700 serves as order of I(S) -n. Similarly, the magnitude of minimum covering T (S) serves as order of I(S) -n. The program identifier p which enables the program of related contents to carry out packaging of them efficiently should be assigned. In an example, a fundamental package is the gestalt of all the program identifiers p that have the bit prefix mu.
[0044] The entitlement of such a single topic package is a single key in the key tree 200. Moreover, a multi-topic package can be assembled without a side effect. Entitlement information is only the set of a key to each TOPICS which consists of a multi-TOPICS package. According to this invention, the package specified by Prefix mu does not force to the set top terminal 400 so that a program may be decoded using zero prefix of the same die length.
[0045] As mentioned above, the head end server 300 performs the program delivery process 800 shown in drawing 8 , and in order to decode a program and to transmit using the program identifier p, he gets the program key kp based on the program identifier p assigned to the program and the master key m. The program delivery process 800 is important for performing in off-line thru/or the real time except an actual transmitting step. As shown in drawing 8 , the program delivery process 800 starts the process using the principle of this invention by identifying the program which should be transmitted (810).
[0046] After that, the program delivery process 800 takes out the program identifier p corresponding to the program from the program database 500 (820), and calculates the program key kp corresponding to the program (830). And a program is enciphered using the program key kp calculated at the front step (840). Finally, the program delivery process 800 transmits the program enciphered with the program identifier p (850), and program control ends it (860).
[0047] It is important to suppose that it is possible to obtain the program key kp required for the program identifier p to be interleaved periodically, able to transmit it through transmission of program information, and for a customer change a channel at the time of a program, and decode a program. In another example, the program identifier p can be continuously transmitted on another control channel like a Barker channel.
[0048] As mentioned above, the set top terminal 400 performs the decoding process 900 shown in drawing 9 , using the entitlement information 600 and the received program identifier p memorized in order to obtain the program key kp, in order to decode the program, the program key kp is used and a customer decodes the program by which the entitlement is carried out. As shown in drawing 9 , the decoding process 900 starts the process which used the principle of this invention on the occasion of the reception of the customer directions made to tune up to a specific channel (910).

[0049] After that, the set top terminal 400 receives the suitable signal containing the enciphered program identifier p which was programmed and transmitted (920). The decoding process 900 takes out the entitlement information memorized from the entitlement database 600 (930). It judges whether the transmitted program is included (940). When the entry which has the partial-program identifier p which agrees in the leftmost digit bit of the receiving-agent identifier p at step 940 is judged not to exist in the entitlement database 600, a customer does not have an entitlement to the selected program and program control is ended (980).
[0050] However, if an entry exists in the entitlement database 600 which has the partial-program identifier p corresponding to the leftmost digit bit of the received program identifier p, a customer has an entitlement to the selected program. Therefore, the program key kp is calculated using the middle key ki taken out from the entry of the entitlement database 600 (960). Specifically, the program key kp is calculated by operating suitable Hash Functions H0 or H1 so that each value of the bit of the low (n-r) order of the program identifier p may direct as follows.
[Equation 5]
$$K_p = H_{p_n}(\ldots H_{p_{r+1}}(H_{p_r}(K_I))\ldots)$$

[0051] Finally, the program is decoded using the obtained program key kp (970), and ends program control (980). When the received program is not a part of a customer's entitlement here, it is important that there is no entitlement information which has the partial identifier p corresponding to the low bit of the program identifier p which received with the transmitting program in the entitlement database 600.
[0052] The decoding process 900 obtains a decode key, or moreover, as mentioned above Before a customer judges whether there is any entitlement to a demand channel In order that it can wait for a customer to demand a specific channel and the decoding process 900 may obtain the transmitting program identifier p instead, all channels are scanned periodically. It is important that the decode key to the storage in data storage 420 can be obtained, and a customer's entitlement can be judged beforehand again.
[0053] a suitable Hash Function -- as mentioned above, if Hash Function H is a pseudo-random bit generation machine, it can prove that mapping of p->kp is a pseudo-random function. Therefore, a code key cannot be predicted if actual Hash Function H is strong in cryptography. Therefore, if a piracy person has access only to encryption program broadcasting, it will not be able to break through a code in the knowledge about the key generated using the tree method of this invention. Therefore, only one concerns only become ensuring that video encryption algorithm can oppose to a well-known plain text attack.
[0054] Hash Function H should hold two properties. Calculating Input x has that it must be difficult noting that the one half H0 of an image (x) or H1 (x) is given to the 1st to Hash Function H. Though this knows the image of both these one half, it is actually materialized also to the cryptography-hash [which] H with it difficult [to carry out an inverted arch]. Moreover, though H1 (x) was known, it must be difficult to calculate H0 (x), and the reverse of a thing is also the same. Even if it is difficult fundamentally to carry out the inverted arch of the function H, when the key of one one half is known, it becomes easier to complete the key of the remaining one half. If that is right, the piracy person who knows Program kp to Node u can calculate the key to the SHIBURINGU (sibling: sibling) node v, and can calculate the key to all the programs in the subtree of Node v.
[0055] As one advantage of the tree method according to this invention, merge of an entitlement carried out in piracy may be made in inefficient. Pair p1, p2, and those ********** of a SHIBURINGU program are considered. A piracy person assumes that the program key kp corresponding to the programs p1 and p2 of both which are two one half of H (kp (u)) is known. A piracy person still cannot do the inverted arch of the H, and cannot calculate kp (u). It is because H is a cryptography-Hash Function. Therefore, the entitlement carried out in the merged piracy must contain both kp (p1) and kp (p2) instead of compact kp (u). therefore, it is not a strategy good for a piracy person to divide to two or more set top terminals 400 which use a CHIPU (it is -- although -- it differs) entitlement. It is because a union ****** entitlement becomes very large.
[0056] As mentioned above, the suitable pseudo-random Hash Function is indicated by reference, and O.Goldreich et al. and "How to Construct Random Functions" J.ACM and 33:792-807 (1986).

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] This invention relates to the system which transmits the program decoded with the memorized entitlement information using the program identifier used by the set top terminal, in order to obtain a decode key required to decode a program especially about the system which restricts access to the contents of transmitting programming.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] It is still more important that a service provider like a cable television operator or a digital satellite service operator offers the package of the channel to which a majority of a television viewer's population is satisfied, or a program as the number of channels with an available television viewer increases and the range of the available contents of programming increases in number by such channel. Generally development of the package with which a customer is provided is a marketing function. A service provider is wanted to offer the package of various sizes generally. For example, they are all programs, the combination between them, etc. from one program.

[0003] A service provider usually broadcasts a television program from the transmitter called a "head end" to many customers. Each customer is usually concerned with a part of programming to receive. For example, in a broadcast environment, any man can receive programming transmitted with a suitable receiver like an antenna or a satellite disk. In order to restrict access of a program only to the normal customer who purchased the package, a service provider usually enciphers a transmitting program and contains 1 or two or more code machines in a customer. A set top terminal (STT) is offered. By such approach, a set top terminal receives encryption transmission and the program which a customer looks at is enciphered. Nothing is carried out but this.
[0004] In order that the confidentiality memorized in the set top terminal may make piracy of high information min, a set top terminal is usually equipped with a secure processor or secure memory. This secure memory has the capacity of several kilobits order, and memorizes a code key. Generally secure memory is not volatility but tamper REJISUTANTO. Moreover, secure memory has that it can write [much] in and can carry out the repro gram of the key for every accounting period. Since the secure memory capacity of the conventional set top terminal is restricted, the number of the keys memorized will be restricted and the number of the packages which a service provider offers will also be restricted. The number of the programs which a service provider broadcasts to the accounting period of a moon unit may usually be the order of 200,000.
[0005] The conventional set top terminal has a thing containing bit VEKUTORU which has a bit entry corresponding to each package of the program which a service provider offers. If a specific customer is the normal addressee of a package, the bit entry in the bit vector memorized in a set top terminal will be set to "1." After that, all the programs that a service provider transmits are enciphered by one key. If a program is received, a set top terminal will judge whether the bit entry which accesses and corresponds to a bit vector is set. If the bit entry is set, as for a set top terminal, a program will be decoded using one memorized code machine.
[0006] Although it seems to a theory top that flexibility is attained by the bit vector method by offering one bit entry to each package (a package consisting of one program generally), the die length of a bit vector is not practical in the system which transmits many programs to one accounting period. Moreover, the access control in such a system is exclusively given by the entry in a bit vector, and is not code-like (cryptographic). Therefore, if a customer can write in a bit vector and can set all bits to "1", a customer will be able to access all programs.
[0007] Moreover, a program is divided into each package and there are some as which all the programs in a package are enciphered using the same key. Each package corresponds to one television channel. A set top terminal memorizes the decode key to each package the customer of whose is a normal addressee. Therefore, if a program is included in two or more packages, that program must be broadcast again for corresponding each package of every, and will be enciphered in this the transmission of each by the code key corresponding to a specific package. Although it is cryptography-like [an access control], by the overhead about broadcasting programming again repeatedly, it will not be realistic, and will carry out arranging the same program as much packages, and flexibility will be restricted in the design of the package of a program.
[0008] although the conventional system which encipher such contents of a program and be transmit be

comparatively successful about restrict access only to a normal customer , it have not make it possible to provide a customer with the package with which a large number which include much programs , without make an overhead increase fairly differ , without a service provider like a television network exceed the secure memory capacity to which the set top terminal be restricted . The cryptography-approach and equipment which restrict access to the contents of transmitting programming to the "Vspace system" indicated by the United States patent applications 08/912186 (August 15, 1997 application) are indicated.

[0009] Each program in a Vspace system is enciphered by the head end server before transmission using the program key kP. Each program key is the linearity combination of the set with which the master key M was defined. The program identifier which identifies a program is transmitted with the contents of encryption programming. A customer's set top terminal can obtain a decode key only from the entitlement information recorded on the program identifier p which received, and the front. A Vspace system offers a cryptography-access-control mechanism, enabling the package which is supple, without extending a program header fairly (only a program identifier being transmitted with a program). It is because it is not necessary to broadcast a program again for corresponding each package of every.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] Generally, the contents of programming enciphered by 1 or two or more customers by the service provider using the transmitter thru/or the head end server are transmitted. The program identifier p used for identifying a program is transmitted to a customer with the contents of programming. Each customer has other devices in which access restricted to transmitting multimedia information using the set top terminal thru/or the decode key is given. A set top terminal receives 1 which can receive to normal at a period with a customer, or the entitlement information corresponding to the package of two or more programs from a head end.
[0011] Each program is enciphered by the head end server before transmission using the program key kp. the program key kp of an individual -- the program -- unique -- making . In addition to transmission of the enciphered program, a head end server transmits the program identifier p to a set top terminal. A set top terminal obtains a decode key required to decode a program using the program identifier p which received with the memorized entitlement information. In this approach, if a customer is the normal user of a specific program, a set top terminal can obtain the program key kp enciphered using the information memorized and received, and can decode the program enciphered using that program key kp after that. In an example, the program identifier p can be interleaved to a part of program, and can be transmitted on a separate exclusive control channel.
[0012] Each of k-bit program key kp used for enciphering a transmitting program can be obtained by applying 1 or two or more pseudo-random Hash Functions to a master key m. As an example, Hash Function H which doubles die length can be used. Therefore, Hash Function H takes a k bit binary value, and makes the binary value of the die length of 2k. The output of Hash Function H can be expressed as pair H0 of k-bit binary value as H1. Here, H0 can be identified as a left half of the output of the Hash Function concerned, and H1 can be identified as a right half of the output of the Hash Function concerned.
[0013] As an example, the program key kp can be obtained according to the binary value to which each bit position of the program identifier p corresponds by applying recurrently Hash Functions H0 or H1 to a master key. Therefore, if the program identifier p consists of m bits, one side of Hash Functions H0 or H1 will be applied to each bit position of n of the program identifier p according to the bit value to which the program identifier p corresponds. First, one side of Hash Functions H0 or H1 is applied to a master key according to the binary value which is the leftmost digit bit of the program identifier p. After that, according to the binary value of a corresponding bit, one side of Hash Functions H0 or H1 is applied to the result of a pre- hash operation to each remaining bit position (n-1). Count of the program key kp can be expressed as follows.
[Equation 1]

$$K_p = H_{p_n}(\ldots H_{p_2}(H_{p_1}(m))\ldots)$$

[0014] Such a hash operation can be expressed in relation to n level binary tree T (called a key tree) by which the root 2 master key m of a tree is arranged. A tree is generable by applying Hash Functions H0 and H1 to each node until a desired number of tree-level (n) is made. The program key kp corresponds to the leaf (leaf) node in the bottom (bottom) level of a tree. The binary index (the same the program identifier [And] p) corresponding to each program key kp corresponds to the pass (way) which passes along the key tree from the root to a desired leaf node. Therefore, the index thru/or label of Node u is connection of the label on H on the pass from the root to Node u. T (u) can calculate any key of the program in subtree T (u) by carrying out time (n-r) actuation of the Hash Function to the internal node u (u1, ..., ur) in depth r in the subtree which makes Node u the root, i.e., the key tree which has the partial program identifier p showing the set of the program identifier p corresponding to the leaf in the subtree of Node u.

[0015]
[Embodiment of the Invention] Drawing 1 has shown the network environment which transmits video, an audio, and encryption multimedia information like data to 1 or two or more customers who have the set top terminals 400-401 through 1 or two or more distribution networks 110 using a transmitter like the head end server 300 from a service provider. This head end server 300 argues in relation to drawing 3 in the bottom, and argues about the set top terminal 400 in relation to drawing 4 in the bottom. In this specification, a set top terminal includes any device in which access restriction is given to the multimedia information transmitted using the decode key. For example, a computer configuration and a communication link device are included. A service provider may download the software which a set top terminal performs. A network 110 can be made into the wireless broadcasting network which distributes contents of programming like digital satellite service (DSSTM), a cable television network (CATV), a public switching network (PSTN), an optical network, ISDN, and a cable network like the Internet.
[0016] The set top terminal 400 receives entitlement information intermittently from the head end server 300, and enables a customer to access the program whose customer is a registered user between a certain time intervals (for example, accounting period). In this specification, a package is the set of a predetermined program and a certain program can belong to 1 or two or more packages. A program means all of continuous multimedia transmission of the episode of television, or specific die length like a movie. Entitlement information is downloadable in the set top terminal 400 from the head end server 300 using which suitable secure one way or bidirectional protocol.
[0017] Program key and program identifier each transmitting program is enciphered by the head end server 300 using the program key kp. This program key kp can be made unique to a program. Suitable encryption and a security technique are indicated by reference, B.Schneier, and Applied Cryptography (2d ed.1997). In addition to transmission of an encryption program, the head end server 300 also transmits a n bit program identifier to the set top terminal 400. This is used by the set top terminal 400 with the memorized entitled information, and as shown in a detail, it obtains a decode key required to decode a program in the bottom.
[0018] The program identifier p is not chosen as arbitration so that the item of the bottom entitled assignment of the program identifier to a program may explain. In a desirable example, the program identifier p can consist of the 32-bit value transmitted in the ECM field specified to MPEG-2 criterion. In this case, if it is the registered user of the program of specification [a customer], the set top terminal 400 can obtain the program key kp from the information memorized and received, and it can use the program key kp so that an encryption program may be decoded after that.
[0019] According to the further description of this invention, each of the k-bit program key kp used for an encryption transmitting program can be obtained by applying 1 or two or more pseudo-random Hash Functions to a master key m. Explanation of a suitable pseudo-random Hash Function is indicated by reference and O.Goldreich et al. and "How to Construct Random Functions" J.ACM and 33:792-807 (1986).
[0020] As an example, it is secure in cryptography, and the Hash Function which doubles die length is used as follows.
H: {0, 1} k->{0, 1}2k -- here, k is the die length of the program key kp. Therefore, Hash Function H takes the binary value of k bits, and makes the binary value of die-length 2k. The output of this Hash Function H can be expressed as pair H0 of a k bit binary value as H1. Here, H0 is the left-hand side one half (left-hand side digit bit) of the output of Hash Function H, and is H. {1} is the right-hand side one half (right-hand side digit bit) of the output of Hash Function H. H0 and H1 can be called a separate Hash Function.
[0021] If it is k= 160, H can be specified using secret hash standard SHA-1 which is indicated by reference, Secure Hash Standard, National Institute of Standards and Technology, NIST FIPS PUB 180-1, and U.S.Dept.of Commerce (April, 1995). That is, H0 is set to SHA-1 (x||0), and H1 turns into SHA-1 (x||1). Here, 0 and 1 are the bit strings of all the bit strings 1 of 0 altogether, respectively.
[0022] The program key kp can be obtained by applying recurrently 1 or two or more Hash Functions to a master key m according to the binary value of the program identifier p. As an example, the program key kp can be obtained by applying recurrently one side of Hash Functions H0 or H1 to a master key m according to the binary value of each bit position of the program identifier p. Generally, if the program identifier p consists of n bits, according to the bit value to which the program identifier p corresponds, one side of Hash Functions H0 or H1 will be applied to each of the bit position of n of the program identifier p (it starts from a leftmost bit).
[0023] One side of Hash Functions H0 or H1 is first applied to a master key according to the binary value which is a leftmost digit bit. After that, according to the binary value which is the bit to which one side of Hash Functions H0 or H1 corresponds, it is applied to the result of pre- hash actuation to each remaining bit position (n-1). This hash actuation can be expressed as follows so that the item of a title called lower "key tree" may explain.

[Equation 2]
$$K_p = H_{p_n}(\ldots H_{p_2}(H_{p_1}(m))\ldots)$$

[0024] As mentioned above, the head end server 300 transmits the program identifier p with an encryption program. Therefore, if the program identifier p is given, the set top terminal 400 must obtain the program key kp used for decode of a receiving agent. As mentioned above, the program key kp can be obtained by applying recurrently 1 or two or more Hash Functions to a master key m according to the binary value of the program identifier p. The program key kp must be obtained by a customer's set top terminal 400, using indirectly the memorized entitlement information and the program identifier p which received which is explained in the bottom.
[0025] As explained on the key tree, the program key kp can be obtained by using recurrently 1 or two or more Hash Functions for a master key m according to the binary value of the program identifier p. The k-bit single master key m is used. The bit of the program identifier p can be expressed as p= (p1, ..., pn). Here, p1 is a leftmost digit bit and is a rightmost digit bit. The cryptographic key kp to the program which has the program identifier p can be defined as follows.
[Equation 3]
$$K_p = H_{p_n}(\ldots H_{p_2}(H_{p_1}(m))\ldots)$$

[0026] Hash actuation can be expressed as a perfect n level binary tree T like the key tree 200 shown in drawing 2 . The key tree 200 shown in drawing 2 corresponds to the example of mounting which has the program identifier p which consists of a triplet. As shown in drawing 2 , a master key m is arranged on the root 210 of a tree 200. The program key kp corresponds to a leaf node like leaf nodes 240-247. The index corresponding to each program key kp shown in drawing 2 like the index 011 corresponding to the program key kp of the DERIFU node 243 shows the pass which lets the key tree 200 from the root 210 to a leaf node 243 pass. For example, the program key kp of 243 can be obtained by following with the left edge (H0) from the root 210, the right edge (H1) from a node 220, and the right edge (H1) from a node 232. That is, H1 is further applied for H0 to the 2nd hash result. The program key kp011 can be obtained.
[0027] Therefore, the label of a node u like a node 243 is what connected the label on the edge of the pass to Node u from the root 210. The label of each node can be specified by the program identifier p. Since the subtree which makes Node u the root is expressed, T (u) is used (namely, since the set of the program identifier p corresponding to the leaf in the subtree of Node u is expressed). The internal node u in depth r in the key tree 200 has the partial program identifier p (u1, ..., ur), and can calculate the key of which program in subtree T (u) to these. Any key of the program in the subtree of Node u is calculable by carrying out time (n-r) actuation of the Hash Function. Specifically, it uses so that the value of each bit of the low digit of (n-r) of the program identifier p may direct suitable Hash Functions H0 or H1. Therefore, the program key kp corresponding to Node u can function as an entitlement to all the programs in the subtree of Node u.
[0028] If Function H is a pseudo-random generator, mapping kp{0, 1} ->[n] {0, 1} k of the program key which the master key m parameterized is a pseudo-random function. This is indicated by reference, and O.Goldreich et al. and "How toConstruct Random Functions" J.ACM and 33:792-807 (1986).
[0029] System component drawing 3 is the block diagram showing the head end server's 300 AKI theque char. A head end shall be related with the service provider of the arbitration which transmits a television network, a cable employment person, a digital satellite service employment person, or the contents of encryption programming. For example the head end server 300, can mount with RS6000 server which manufactures, and can perform the function and actuation of this invention. The head end server 300 is equipped with related memory like a processor 310 and the data storage device 320. A processor 310 may be mounted as a single processor and may be mounted as some processors which operate to juxtaposition. The data storage device 320 and ROM are made to memorize 1 or two or more instructions, and a processor 310 enables it to perform by taking out and interpreting.
[0030] As mentioned above, the data storage device 320 is equipped with the master key database 350 which memorizes a master key m. For example, a master key m can be updated like [for every accounting period]. Moreover, the data storage device 320 has the program database 500 so that it may explain in relation to drawing 5 in the bottom. The program database 500 presents the program identifier p and the related package corresponding to each program. moreover, drawing 7 R> -- the data storage device 320 has the entitlement information delivery process 700 and the program delivery process 800 so that it may explain in relation to 7 and 8.
[0031] Generally, the entitlement information delivery process 700 generates and distributes the entitlement

information which each customer needs to accessing the program which is a registered user. Moreover, the program delivery process 800 obtains the program key kp based on the program identifier p assigned to the program, in order to encipher a program and to transmit by the program identifier p.
[0032] The communication link port 330 links the head end server 300 to each connected receiver like the set top terminal 400 which showed the head end server 300 to the network 110 at a bond and drawing 1 .
[0033] Drawing 4 is the block diagram showing the AKI theque char of the set top terminal 400. The set top terminal 400 can be mounted as a set top terminal (STT) corresponding to television, and it can be changed so that the function and actuation of this invention may be performed. The set top terminal 400 is equipped with a processor 410 and memory like data storage 420, and the communication link port 430, and operates by the same approach as the above hardware relevant to drawing 3 .
[0034] Data storage 420 is equipped with the entitlement database 600 memorizable into the secure part of data storage 420 so that it may explain in relation to drawing 6 in the bottom. The entitlement database 600 contains the part of the key tree 200 required in order that a customer may get the program key kp to the program which has an entitlement. Moreover, data storage 420 is equipped with Hash Functions H0 and H1 (440). Moreover, data storage 420 includes the decoding process 900 so that it may explain in relation to drawing 9 in the bottom. Generally, using the program identifier p received in order to obtain the program key kp, and the memorized entitlement information 600, in order to decode a program, the program key kp is used for the decoding process 900, and it decodes the program whose customer has an entitlement.
[0035] Drawing 5 shows the program database 500 which memorizes information on each program p transmitted by the head end server 300. This information is transmitted to for example, an accounting period with the program identifier p to which that program belongs and which packs and corresponds. The program database 500 holds two or more decodings like records 505-520. These are related with a different program, respectively. The program database 500 contains the program identifier p which corresponds in the field 535 including directions of the corresponding package with which the program belongs in the field 530 to each program identifier identified by the program name in the field 525.
[0036] Drawing 6 shows the entitlement database 600 containing the part of the key tree 200 required for a customer to get the program key kp to the program which has an entitlement. As mentioned above, T (u) expresses the set of the program identifier p corresponding to the leaf nodes 240-247 in the subtree which makes Node u the root, i.e., the subtree of Node u. For example, supposing a customer has an entitlement about receiving four programs corresponding to leaf nodes 240-243, entitlement information will consist of a middle key corresponding to a node 220. In this approach, if needed, suitable Hash Functions H0 and H1 (440) can be used in order to obtain the program key kp to each nodes 230, 232, 240-243 in the subtree of a node 220.
[0037] The entitlement database 600 shown by drawing 6 is a registered user who receives four programs corresponding to leaf nodes 240-243 (there is an entitlement), and is a registered user who receives two programs corresponding to leaf nodes 246-247. Therefore, the entitlement information recorded on the entitlement database 600 consists of a middle key corresponding to a node 220 and a node 236. nodes 220 and 236 -- it is alike, respectively, and it receives, and the entitlement information recorded on the entitlement database 600 has the middle key values kio and ki11, respectively, and has corresponding directions of the partial program identifier p. The approach by which the entitlement database 600 is generated by the entitlement information delivery process 700 based on the package of the program which the customer chose is explained in relation to drawing 7 in the bottom.
[0038] A small entitlement is establishable to the set of many programs of various sizes using the tree method of program packaging this invention. The target set S is established using the set of the program packed. The minimum set of a tree node with which a subtree covers the target set S correctly is obtained as follows.
[Equation 4]
$T(S)=Z\subseteq T$ ただし、$\bigcup_{u\in Z}T(u)=S$ 、かつ、$|Z|$ は最小であるように

[0039] The entitlement information over Package S is the set ki of the middle key held in the node of T (S). As shown in a top, the set top terminal 400 decodes the program in S (accepting it) correctly with the set of this key. Theoretically, the tree method of this invention can build the entitlement information over the target set S of which arbitration. furthermore -- however, if the program identifier p is assigned to arbitration, entitlement information will become so large that it is not allowed for the secure memory to which the set top terminal 400 was restricted.
[0040] a process -- as mentioned above, the head end server 300 performs the entitlement information delivery

process 700 shown in drawing 7 , and generates and distributes the entitlement database 600 required for each user in order to access the program which is a registered user. As mentioned above, the entitlement database 600 consists of corresponding directions and the corresponding middle key value ki of a partial program identifier to each node of the key tree 200 required for a customer to get the program key kp to the program which is a registered user.
[0041] Therefore, the entitlement information delivery process 700 identifies first the program which the customer chose (710). After that, the entitlement information delivery process 700 finds minimum set [of a tree node] T (S). The subtree covers the target set S correctly. The target set S is disassembled to the maximum De Dis joint interval of the KONSEKYUTIBU program identifier p (720). Two program identifiers p are considered to be KONSEKYUTIBU when the integer over the binary expression is KONSEKYUTIBU.
[0042] And covering T (S) is found to each interval (730). The corresponding partial program identifier p held in the node of covering T (S) to Set ki and each interval of a middle key is generated (740). At the end, the generated entitlement information downloads to the set top terminal 400 with the head end server 300 (750), and program control is completed (760).
[0043] The number of the intervals in the target set S can be set to I (S). In order to calculate covering T (S) to the single interval of the program identifier p to the order of the tree node of n, the key tree 200 of depth n must be asked. Therefore, the time amount complexity of the entitlement information delivery process 700 serves as order of I(S) -n. Similarly, the magnitude of minimum covering T (S) serves as order of I(S) -n. The program identifier p which enables the program of related contents to carry out packaging of them efficiently should be assigned. In an example, a fundamental package is the gestalt of all the program identifiers p that have the bit prefix mu.
[0044] The entitlement of such a single topic package is a single key in the key tree 200. Moreover, a multi-topic package can be assembled without a side effect. Entitlement information is only the set of a key to each TOPICS which consists of a multi-TOPICS package. According to this invention, the package specified by Prefix mu does not force to the set top terminal 400 so that a program may be decoded using zero prefix of the same die length.
[0045] As mentioned above, the head end server 300 performs the program delivery process 800 shown in drawing 8 , and in order to decode a program and to transmit using the program identifier p, he gets the program key kp based on the program identifier p assigned to the program and the master key m. The program delivery process 800 is important for performing in off-line thru/or the real time except an actual transmitting step. As shown in drawing 8 , the program delivery process 800 starts the process using the principle of this invention by identifying the program which should be transmitted (810).
[0046] After that, the program delivery process 800 takes out the program identifier p corresponding to the program from the program database 500 (820), and calculates the program key kp corresponding to the program (830). And a program is enciphered using the program key kp calculated at the front step (840). Finally, the program delivery process 800 transmits the program enciphered with the program identifier p (850), and program control ends it (860).
[0047] It is important to suppose that it is possible to obtain the program key kp required for the program identifier p to be interleaved periodically, able to transmit it through transmission of program information, and for a customer change a channel at the time of a program, and decode a program. In another example, the program identifier p can be continuously transmitted on another control channel like a Barker channel.
[0048] As mentioned above, the set top terminal 400 performs the decoding process 900 shown in drawing 9 , using the entitlement information 600 and the received program identifier p memorized in order to obtain the program key kp, in order to decode the program, the program key kp is used and a customer decodes the program by which the entitlement is carried out. As shown in drawing 9 , the decoding process 900 starts the process which used the principle of this invention on the occasion of the reception of the customer directions made to tune up to a specific channel (910).
[0049] After that, the set top terminal 400 receives the suitable signal containing the enciphered program identifier p which was programmed and transmitted (920). The decoding process 900 takes out the entitlement information memorized from the entitlement database 600 (930). It judges whether the transmitted program is included (940). When the entry which has the partial-program identifier p which agrees in the leftmost digit bit of the receiving-agent identifier p at step 940 is judged not to exist in the entitlement database 600, a customer does not have an entitlement to the selected program and program control is ended (980).
[0050] However, if an entry exists in the entitlement database 600 which has the partial-program identifier p corresponding to the leftmost digit bit of the received program identifier p, a customer has an entitlement to the selected program. Therefore, the program key kp is calculated using the middle key ki taken out from the entry of the entitlement database 600 (960). Specifically, the program key kp is calculated by operating suitable Hash Functions

H0 or H1 so that each value of the bit of the low (n-r) order of the program identifier p may direct as follows.
[Equation 5]
$$K_p = H_{p_n}(\ldots H_{p_{r+1}}(H_{p_r}(K_I))\ldots)$$

[0051] Finally, the program is decoded using the obtained program key kp (970), and ends program control (980). When the received program is not a part of a customer's entitlement here, it is important that there is no entitlement information which has the partial identifier p corresponding to the low bit of the program identifier p which received with the transmitting program in the entitlement database 600.
[0052] The decoding process 900 obtains a decode key, or moreover, as mentioned above Before a customer judges whether there is any entitlement to a demand channel In order that it can wait for a customer to demand a specific channel and the decoding process 900 may obtain the transmitting program identifier p instead, all channels are scanned periodically. It is important that the decode key to the storage in data storage 420 can be obtained, and a customer's entitlement can be judged beforehand again.
[0053] a suitable Hash Function -- as mentioned above, if Hash Function H is a pseudo-random bit generation machine, it can prove that mapping of p->kp is a pseudo-random function. Therefore, a code key cannot be predicted if actual Hash Function H is strong in cryptography. Therefore, if a piracy person has access only to encryption program broadcasting, it will not be able to break through a code in the knowledge about the key generated using the tree method of this invention. Therefore, only one concerns only become ensuring that video encryption algorithm can oppose to a well-known plain text attack.
[0054] Hash Function H should hold two properties. Calculating Input x has that it must be difficult noting that the one half H0 of an image (x) or H1 (x) is given to the 1st to Hash Function H. Though this knows the image of both these one half, it is actually materialized also to the cryptography-hash [which] H with it difficult [to carry out an inverted arch]. Moreover, though H1 (x) was known, it must be difficult to calculate H0 (x), and the reverse of a thing is also the same. Even if it is difficult fundamentally to carry out the inverted arch of the function H, when the key of one one half is known, it becomes easier to complete the key of the remaining one half. If that is right, the piracy person who knows Program kp to Node u can calculate the key to the SHIBURINGU (sibling: sibling) node v, and can calculate the key to all the programs in the subtree of Node v.
[0055] As one advantage of the tree method according to this invention, merge of an entitlement carried out in piracy may be made in inefficient. Pair p1, p2, and those ********** of a SHIBURINGU program are considered. A piracy person assumes that the program key kp corresponding to the programs p1 and p2 of both which are two one half of H (kp (u)) is known. A piracy person still cannot do the inverted arch of the H, and cannot calculate kp (u). It is because H is a cryptography-Hash Function. Therefore, the entitlement carried out in the merged piracy must contain both kp (p1) and kp (p2) instead of compact kp (u). therefore, it is not a strategy good for a piracy person to divide to two or more set top terminals 400 which use a CHIPU (it is -- although -- it differs) entitlement. It is because a union ****** entitlement becomes very large.
[0056] As mentioned above, the suitable pseudo-random Hash Function is indicated by reference, and O.Goldreich et al. and "How to Construct Random Functions" J.ACM and 33:792-807 (1986).

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram showing the system which transmits the enciphered contents of programming according to one example of this invention.
[Drawing 2] Drawing showing the example of the key tree according to this invention.
[Drawing 3] The block diagram of the head end server of drawing 1 .
[Drawing 4] The block diagram of the set top terminal of drawing 1 .
[Drawing 5] The table from the program database of drawing 3 .
[Drawing 6] The table from the entitled database of drawing 4 .
[Drawing 7] The flow chart showing the entitlement information delivery process which the head end server of drawing 3 uses.
[Drawing 8] The block diagram showing the program distribution flow chart which the head end server of drawing 3 uses.
[Drawing 9] The flow chart showing the record process which the set top terminal of drawing 4 uses.
[Description of Notations]
110 Distribution Network
200 Key Tree
220, 230, 232, 236, 240-243, 246-247 Node
300 Head End Server
310 410 Processor
320 420 Data storage
350 databases
330 430 Communication link port
400-401 Set top terminal
440 Hash Functions H0 and H1
500 Program Database
505-520 Decoding
525, 530, 535 Field
600 Entitlement Database
700 Entitlement Information Delivery Process
710 Identify Program Which Customer Chose.
720 Decompose to the Maximum De Dis Joint Interval of Target Set KONSEKYUTIBU Program Identifier P.
730 Find Covering T (S) to Each Interval.
740 Generate Partial-Program Identifier P to which Middle Key Ki Sets and Corresponds in Node of Covering T (S) to Each Interval.
750 Transmit Entitlement Information to Set Top Terminal.
760, 860, 980 Termination
800 Program Delivery Process
810 Identify Program Which Should be Transmitted.
820 Take Out Program Identifier P from Program Database.
830 Calculate Program Key.
840 Encipher Program Using Program Key.
850 Transmit Program Enciphered with Program Identifier P.

900 Decoding Process
910 Take Out Customer Directions Made to Tune Up to Channel.
920 Receive Sending Signal Containing Program and Program Identifier P.
930 Take Out Entitlement Information Memorized from Entitlement Database.
940 Is There an Entry Which Has Partial-Program Identifier P corresponding to MSB of Receiving-Agent Identifier P?
960 Come Out Picking and Calculate Program Key Kp Using Ki Value and Hash Functions H0 and H1 Bottom.
970 Decode Program Using Program Key Kp.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CORRECTION OR AMENDMENT

[Kind of official gazette] Printing of amendment by the convention of 2 of Article 17 of Patent Law
[Section partition] The 3rd partition of the 7th section
[Publication date] November 8, Heisei 14 (2002. 11.8)

[Publication No.] JP,2001-36517,A (P2001-36517A)
[Date of Publication] February 9, Heisei 13 (2001. 2.9)
[Annual volume number] Open patent official report 13-366
[Application number] Application for patent 2000-135069 (P2000-135069)
[The 7th edition of International Patent Classification]

H04L 9/08
G09C 1/00 650
H04N 5/44
7/08
7/081
7/16
7/167

[FI]

H04L 9/00 601 D
G09C 1/00 650 Z
H04N 5/44 A
7/16 C
H04L 9/00 601 E
H04N 7/08 Z
7/167 Z

[Procedure revision]
[Filing Date] August 13, Heisei 14 (2002. 8.13)
[Procedure amendment 1]
[Document to be Amended] Specification
[Item(s) to be Amended] Claim
[Method of Amendment] Modification
[Proposed Amendment]
[Claim(s)]
[Claim 1] It is the approach of transmitting the program which can carry out access restriction to an end user,
(A) The step which assigns the program identifier which has a binary value to said program,
(B) The step which defines at least one master key,
(C) The step which enciphers said program by using the program key obtained by applying at least one Hash Function to said master key based on the binary value of said program identifier,
(D) The approach characterized by having the step which sends said enciphered program to said end user with said program identifier.
[Claim 2] Said program identifier is an approach according to claim 1 characterized by applying one of said the Hash

Functions to each location of n bits of said program identifier according to the bit value to which it becomes from n bits and said program identifier corresponds.
[Claim 3] (E) The approach according to claim 1 characterized by having further the step which provides said end user with entitlement information based on the set of the program acquired by said end user.
[Claim 4] The approach according to claim 3 characterized by including some key trees based on the set of the program acquired by said end user in said entitlement information.
[Claim 5] Said end user is an approach according to claim 3 characterized by using said program identifier in order to obtain said program key from said memorized entitlement information.
[Claim 6] Said program identifier is an approach according to claim 1 characterized by interleaving with transmission of said encryption program.
[Claim 7] Said program identifier is an approach according to claim 1 characterized by being transmitted on a control channel.
[Claim 8] It is the approach of transmitting a program to two or more end users,
(A) The step enciphered using the program key obtained by applying a Hash Function to the master key based on the binary value of each bit position of said program identifier for the program which has a program identifier recurrently,

(B) The approach characterized by having the step which transmits the enciphered program and said program identifier to said end user.
[Claim 9] It is the approach of transmitting the program corresponding to at least one program package to two or more end users,
(A) The step which provides said end user with entitlement information based on the set of the program acquired by said end user,
(B) The step enciphered using the program key obtained by applying a Hash Function to the master key based on the binary value of each bit position of said program identifier for the program which has a program identifier recurrently,

(C) It has further the step which transmits said program identifier to said end user with the enciphered program,
It is the approach characterized by obtaining said program key from the entitlement information said end user was remembered to be when said end user was a just user of said program.
[Claim 10] It is the approach of decoding the enciphered program,
(A) The step which receives the entitlement information which contains at least one middle key from a key tree based on the set of the program which said customer acquired from the provider of said program,
(B) The encryption program enciphered by the program key, and the step which receives a program identifier,
(C) The step which obtains said program key from the part said program identifier and said key tree were remembered to be,
(D) The approach characterized by having the step which decodes said encryption program using said program key.
[Claim 11] Said program identifier consists of n bits,
It is the approach according to claim 10 which said master key is arranged on the root of said key tree, and is characterized by generating said key tree when said key tree applies a Hash Function to each node until the tree level of n is made.
[Claim 12] It is the approach of decoding the enciphered program,
(A) The step which receives the entitlement information which contains at least one middle key from the key tree based on the set of the program which a customer acquires from the provider of said program,
(B) The encryption program enciphered by the program key, and the step which receives a program identifier,
(C) The step which obtains said program key from the part the key tree was remembered to be from said program identifier and said middle key by applying a Hash Function to said middle key recurrently based on the binary value of said program identifier,
(D) The approach characterized by having the step which decodes said encryption program using said program key.
[Claim 13] Said program identifier consists of n bits,
It is the approach according to claim 12 which said middle key corresponds to the intermediate node in the level r of said key tree, and is characterized by carrying out n-r time application of said Hash Function at said middle key.
[Claim 14] It is the system which transmits the program which restricts access to an end user,
(A) Memory which memorizes a master key and a computer readout possible code,
(B) It has the processor connected with said memory in actuation, and this processor,
(a) Assign the program identifier which has a binary value to said program,

(b) Define at least one master key,
(c) Encipher said program using a program key by applying at least one Hash Function to said master key based on the binary value of said program identifier,
(d) The system characterized by constituting so that an encryption program may be transmitted to said end user with said program identifier.
[Claim 15] It is the system which transmits the program to which access to an end user was restricted,
(A) Memory which memorizes a master key and the code which can be computer read,
(B) It has the processor connected with said memory on actuation,
Said processor,
(a) Encipher this program that has a program identifier using the program key obtained by applying a Hash Function to a master key recurrently based on the binary value of each bit position of said program identifier,
(b) The system characterized by constituting so that this program enciphered by said end user and said program identifier may be transmitted.
[Claim 16] It is the system which decodes the enciphered program,
(A) Memory which memorizes a master key and the code which can be computer read,
(B) It has the processor connected with said memory on actuation, and is said processor,
(a) Receive the entitlement information containing the part of the key tree based on the set of the program acquired by said customer from the provider of this program,
(b) Receive the encryption program enciphered by the program key and a program identifier,
(c) Obtain said program key from said part said program identifier and said key tree were remembered to be,
(d) The system characterized by constituting so that said encryption program may be decoded using said program key.

[Claim 17] It is the medium by which the code means which can be computer read was mounted and which can be computer read, and this means that can be computer read is at the time of operation,
(a) Assign the program identifier which has a binary value to a program,
(b) Define at least one master key,
(c) Encipher this program using the program key obtained by applying at least one Hash Function to said master key based on the binary value of said program identifier,
(d) The medium which is characterized by transmitting this program enciphered with said program identifier to an end user and which can be computer read.
[Claim 18] It is the medium by which the code means which can be computer read was mounted and which can be computer read, and this means that can be computer read is at the time of operation,
(a) Receive the entitlement information containing the part of the key tree based on the set of the program acquired by said customer from the provider of this program,
(b) Receive the encryption program enciphered by the program key and a program identifier,
(c) Obtain said program key from said part said program identifier and said key tree were remembered to be,
(d) The medium which is characterized by decoding said encryption program using said program key and which can be computer read.

[Translation done.]